TASK ORDER REQUEST (TOR)

47QFCA21F0001

Revolutionary Information Technology Services (RITS)

in support of the:

United States Army Corps of Engineers (USACE) Office of the Chief Information Officer (OCIO/G-6)

Issued to:
Science Applications International Corporation (SAIC)
(GSA) Alliant 2 Unrestricted Governmentwide Acquisition Contract (GWAC), Multiple Award, Indefinite Quantity (IDIQ) Contract

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

November 30, 2020

FEDSIM Project Number CR0182

C.1 BACKGROUND

The mission of the United States Army Corps of Engineers (USACE) is to deliver vital public and military engineering services in peace and in war to strengthen the nation's security, energize the economy, and reduce risks from disasters.

USACE is a Federal agency and an Army Direct Reporting Unit made up of approximately 37,000 dedicated civilians and soldiers delivering engineering services to customers in more than 90 countries worldwide, making it the world's largest public engineering, design, and construction management agency. Reference: **(Section J, Attachment Z)** USACE Location List. USACE provides vital public services to millions of United States (U.S.) residents, and its operational capability safeguards human lives and trillions of dollars in land and private property assets. While generally associated with dams, canals, and flood protection in the U.S., USACE is also involved in a wide range of public works support to the nation and the Department of Defense (DoD) throughout the world. The USACE is the nation's number one provider of outdoor recreation and provides 24 percent of the U.S. hydropower capacity. USACE military and civilian engineers, scientists, and other specialists are also leaders of engineering and environmental missions. This diverse workforce of engineers, geologists, hydrologists, biologists, natural resource managers, and other professionals meets the demands of changing times and requirements as a vital part of the U.S. Army.

USACE provides quality, responsive engineering services to the nation, which include:

a. Planning, designing, building, and operating water resources and other civil works projects (navigation, flood control, environmental protection, wetlands regulation, and disaster response).
b. Designing and managing the construction of military facilities for the Army and Air Force (military construction).
c. Providing support to the Federal Emergency Management Agency (FEMA) and other Federal, state, local, and tribal entities during national and natural Emergency Response and Recovery Operations.
d. Surveying, acquiring, managing, condemning, and disposing of real estate for authorized Government customers.
e. Providing design and construction management services for other Federal agencies.
f. Planning, designing, building, and operating locks and dams. Other civil engineering projects include flood control, beach nourishment, and dredging for waterway navigation.
g. Environmental regulation and ecosystems restoration.
h. Maintaining more than 12,000 miles (19,000 kilometers) of commercially navigable channels across the U.S.

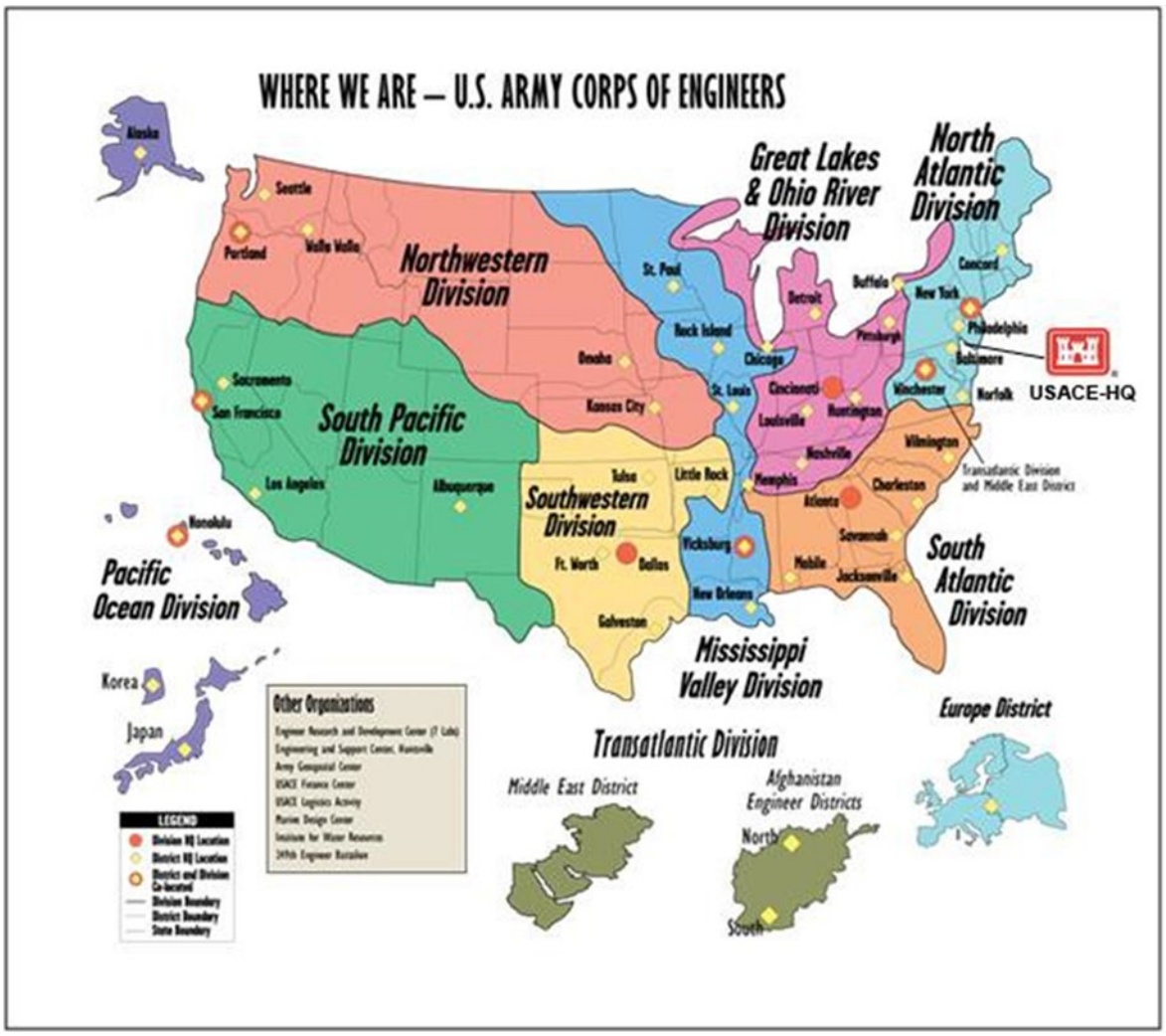

Figure 1. USACE Locations

C.1.1 PURPOSE

The purpose of this requirement is to provide a modern and secure enterprise-wide IT support services to approximately 37,000 USACE customers located throughout the Continental United States (CONUS) and Outside the Continental United States (OCONUS). Services identified as part of this requirement will support the mission needs of USACE's Headquarters (HQs) located in Washington, D.C., nine Divisions **(Reference Figure 1. USACE Locations)**, and 43 Districts, to include over 1,500 field and area project offices and two data centers that are currently located in Vicksburg, Mississippi, and Hillsboro, Oregon.

C.1.2 AGENCY MISSION

The USACE Office of the Chief Information Officer (OCIO)/G-6 is led by the Chief Information Officer (CIO), who provides executive leadership and execution of the USACE Information Management and Information Technology (IM/IT) program.

The USACE OCIO/G-6 is composed of two primary elements: 1) the OCIO, which performs the staff functions of governance, architectural compliance and control, policy development and enforcement, portfolio management, and budget development and review; and 2) the G-6, which provides the line functions of delivering secure IM/IT services to USACE.

The OCIO/G-6 vision and direction is to be an agile, modern mission partner providing world-class IM/IT services that are secure, available, and reliable, while delivering responsive and dependable customer support exceeding expectations of USACE end users. The USACE OCIO/G-6 aims to achieve this vision by engaging mission partners and strategically forecasting future needs, to ensure desired world-class results are accomplished on time and under budget. The OCIO/G-6 seeks to support and modernize IT capabilities essential to the USACE mission through readily available, reliable, and secure network service wherever and whenever needed, as well as to continuously improve IM/IT service responsiveness and systems availability to ensure optimal customer experiences.

OCIO/G-6 provides the following enterprise-wide IM/IT services for USACE and its end users:

a. Automation
b. Communication
c. Communication Security (COMSEC) Support
d. Cyber Security (to include Information Assurance (IA))
e. Data Center Operations Support
f. Emergency Response
g. Enterprise Database Management
h. Enterprise Email Support
i. Enterprise Service Desk
j. Engineering Design Services for Local and Enterprise Requirements
k. Forms Management
l. Automated Information System (AIS) Development
m. Personal Computer (PC) Desktop Local Support
n. PC Lifecycle Management
o. Print Services Liaison
p. Project Management
q. Publication Management
r. Records Management
s. Regional IT Management
t. Service Management
u. Software Support
v. Telephone (Wired and Voice over Internet Protocol (VoIP))
w. Visual Information
x. Video Teleconference (VTC) Support
y. Web and SharePoint Support
z. Wireless Device Support

aa. Mail Peripherals

bb. Supervisory Control And Data Acquisition (SCADA), Industrial Control Systems (ICS) and Operational Technology (OT) solutions

C.2 SCOPE

The scope of the TO is to provide enterprise IT services for the USACE. The contractor shall provide technical support capabilities, including program management, IT infrastructure and shared services, general IT, cybersecurity services, engineering design, telecommunications services, emergency response, transformation, and surge/special projects capability and support. Under the oversight of and in collaboration with USACE OCIO/G-6, the contractor shall execute IT service delivery and transformation.

The contractor shall utilize Information Technology Infrastructure Library (ITIL) practices for IT Service Management (ITSM) that focuses on solutions that have an integrated, enterprise-wide focus to deliver shared IT services that align USACE OCIO/G-6 services with the needs of its customers and end users.

The places of performance for these IT services shall be at multiple locations within CONUS and OCONUS (e.g., the territories of Guam, the Virgin Islands, and Puerto Rico, and Korea, Japan, and Germany).

C.3 CURRENT INFORMATION TECHNOLOGY (IT) NETWORK ENVIRONMENT

USACE OCIO/G-6 is responsible for over 130,000 IT systems, governed by a variety of management controls including Investment Review Boards and Change Control Boards. These systems are diverse and have often been tailored to meet the Government's requirements.

USACE's current environment includes approximately 20,750 servers, network devices, firewalls, appliances, and printers; 32,900 VOIP devices; 40,000 laptops, tablets, and workstations; approximately 60,000 telephone numbers and telephones; 13,000 mobile devices; Supervisory Control and Data Acquisition (SCADA) and Operational Technology (OT) equipment; and other end-user devices. The total number of devices supporting mobility is expected to slowly increase over time. Reference: **(Section J, Attachment Y)** USACE Hardware and Software List.

There are approximately 2.5 million Internet Protocol (IP) addresses across three class B networks plus some smaller networks on a continuous basis using network access control tools. These networks and devices are distributed across approximately 1,650 different locations and sites.

The contractor shall seamlessly assume the current USACE environment to maintain and operate existing systems. After Task Order Award (TOA), the contractor shall work with the Government to begin the transformation process.

USACE OCIO/G-6 currently utilizes Microsoft (MS), Amazon Web Services (AWS), and Oracle cloud services and intends to increase cloud presence during performance of this TO

The strategic USACE OCIO/G-6 IT direction will shift IT delivery from a decentralized, primarily Government-owned, contractor-operated, stove-piped approach to a business model

that has an integrated, enterprise-wide focus supporting a mix of Government-owned, contractor-operated and contractor-owned, contractor-operated environments. This model employs a portfolio-based approach that delivers shared services using an established governance structure.

C.4 OBJECTIVE

The objective of this TO is to assist the USACE OCIO/G-6 with its goals by providing agile, innovative, customer-focused and cost-effective integrated enterprise IT support services in support of USACE's mission of engineering solutions for the nation's toughest challenges. This TO shall provide enterprise IT solutions to enhance and strengthen USACE's IT foundation and deliver secure, revolutionary, and modernized technological solutions to end users and customers.

The proposed strategic USACE OCIO/G-6 IT direction will shift IT delivery from a decentralized, stove-piped approach to a business model that has an integrated, enterprise-wide focus including contractor-owned, contractor operated solutions as recommended by the contractor and approved by the Government. This model employs a portfolio-based approach that delivers shared services using an established governance structure.

USACE OCIO/G-6 is aligning its IT capabilities to provide enterprise service delivery and evolve infrastructure and service delivery from its current state to a modern service delivery model. This new model will increasingly rely on contractor-provided devices and infrastructure to enhance the end-user experience and to support the vital USACE mission of delivering engineering solutions.

The contractor shall provide integrated, consumption based, IT support services for the USACE enterprise bolstering the end-user experience. The contractor shall leverage technology and business processes to build synergies across the enterprise, develop and maintain consistency in process and procedures, and increase mission capabilities of USACE end users.

The contractor shall support USACE OCIO/G-6 through successful performance of the following high-level objectives:

a. Continual modernization of USACE's portfolio of IT systems and ensure USACE remains a leader in cybersecurity compliance, positive audit results, patching speed, and security innovation.
b. Deliver enterprise-wide IT solutions that are well-integrated, flexible, and adaptable across all IT service areas, with the ability to rapidly scale in response to USACE dynamic business environment.
c. Support a geographically dispersed workforce and deploy greater coverage at remote sites to increase the use of real-time tools. USACE seeks to modernize its IT systems and infrastructure by providing field offices with upgraded IT support.
d. Develop a balance between delivering tactical support (operations and maintenance) and strategic support (development, modernization, and enhancement) that achieves operational and cost efficiencies while positioning USACE stakeholders and end users to fulfill their mission.

e. Deploy IT services appropriately to the identified need with the ability to apportion charges to internal and external clients according to use. (A functioning, equitable, and transparent service charge-back mechanism in place across the enterprise.)
f. Maintain a secure environment that includes necessary authorization and authentication, which adequately protects privacy information.
g. Provide service cost and other service management details to ensure USACE remains a leader in technology management, exceeding the expectations set forth by the Office of Management and Budget's (OMB's) annual Federal Information Security Management Act (FISMA) objectives, as well as providing cost transparency to the USACE CIO G/6 customer base.

C.5 TASKS

a. Task 1 – Program Management
b. Task 2 – Enterprise Shared Services
c. Task 3 – General IT Support
d. Task 4 – Cybersecurity
e. Task 5 – Telecommunications
f. Task 6 – Transformation
g. Task 7 – Emergency Response (Optional)

C.5.1 TASK 1 – PROGRAM MANAGEMENT SUPPORT

The contractor shall provide program management support under this requirement. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

The contractor's governance structure shall be scalable to effectively support an enterprise environment: defined as a singular organization derived from multiple funding entities with the need to separately track project management and contract elements such as requirements, deliverables, costs, and ceiling. The Government will utilize the term Technical Direction Letter (TDL) to identify and track operational support needs. These TDLs will be initiated at varying times within the PoP, vary from enterprise-wide to local site requirements, and consist of various appropriation types (e.g., one-year, two-year, no-year, etc.) depending on the bona fide need. These efforts are severable in nature, impacting the level of tracking required to ensure that the Government maximizes the availability of funds.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this Contract for the USACE via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs shall be for the labor executed during the PoP during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROGRAM KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Program Kick-Off Meeting at the location approved by the Government **(Section F, Deliverable 01)**. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, the USACE Technical Point of Contact (TPOC), other relevant Government personnel, and the FEDSIM COR.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda **(Section F, Deliverable 02)** for review and approval by the FEDSIM COR and the USACE TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Introduction of team members and personnel to include roles, responsibilities, and lines of communication, including Points of Contact (POCs), between the contractor and the Government.
b. Staffing Plan and status.
c. Transition-In Plan **(Section F, Deliverable 03)** and discussion.
d. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
e. Financial forecasting/tracking and invoicing requirements
f. TDL management process.
g. Project Management Plan (PMP) discussion including schedule, tasks, etc.
h. Baseline Quality Management Plan (QMP) **(Section F, Deliverable 04)**.
i. Service Integration and Management (SIAM) plan **(Section F, Deliverable 05)**.
j. Cyber Security Management Plan (CSM) **(Section F, Deliverable 06)**
k. Proposed Task Order (TO) Portal **(Section F, Deliverable 07)**

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report **(Section F, Deliverable 08)** documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PROGRAM MANAGEMENT REVIEW (PMR)

The contractor shall develop and provide a monthly PMR **(Section J, Attachment F) (Section F, Deliverable 09).** The PMR shall include the following:

a. Activities during reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities) by TDL. Each section shall start with a brief description of the task.
b. Report system outages and impact on uptime/availability percentages.
c. Report services' performance outside of tolerance thresholds.
d. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
e. Updated Personnel Roster that includes all contractor personnel (including subcontractors and teaming partners) by location, project, ALLIANT 2 labor category, and functional role. The roster shall also specifically identify any gains, losses, and status changes (e.g., security clearance).
f. Government actions required.
g. Schedule (show major tasks, milestones, and deliverables, and planned and actual start and completion dates for each).
h. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the PMR for reporting period).
i. Detailed cost accounting by CLIN, Task, Subtask, ACE Work Center and/or TDL.
j. Costs incurred by CLIN, Task and Subtask, ACE Work Center and/or TDL Costs incurred but not billed by CLIN, Task and Subtask, ACE Work Center and/or TDL
k. Accumulated invoiced cost for each CLIN, Task, Subtask, ACE Work Center and/or TDL up to the previous month.
l. Estimate at completion for each CLIN, Task and Subtask, ACE Work Center and/or TDL
m. Variance at completion based on funding availability for each CLIN, Task and Subtask, ACE work Center and/or TDL.
n. Updates for USACE CIO/G6 service areas supported

The contractor Program Manager (PM) shall convene a monthly Program Review Meeting with the USACE TPOC, FEDSIM Contracting Officer's Representative (COR), and other Government stakeholders (**Section F, Deliverable 10)**. The purpose of this meeting is to ensure all stakeholders are informed of the technical monthly activities and PMR, provide opportunities to identify other activities and establish priorities, provide updates on program financials and identify any financial issues, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (**Section F, Deliverable 11)**.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL EXCHANGE MEETINGS

The contractor shall convene Technical Exchange Meetings with individual service-level components and other Government stakeholders as required. The Technical Exchange Meetings shall provide an opportunity for the contractor and service-level components to review the status of services being provided. The contractor shall provide minutes of these meetings when requested by the Government, including attendance, issues discussed, decisions made, and action items assigned, to the USACE TPOC and FEDSIM COR within two workdays following the meeting (**Section F, Deliverable 12)**.

C.5.1.5 SUBTASK 5 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP and shall provide it to the Government (**Section F, Deliverable 13)**.

The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for TO tasks and service delivery.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS).
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, and other rules of engagement between the contractor and the Government.
g. Contain a Communication Plan to identify and track all required communications as part of the PMP, which identifies all key stakeholders and appropriate communications formats (e.g., meetings and briefings), content, and schedules for each stakeholder.
h. Include the contractor's QMP.

The PMP is evolutionary documents that shall be updated annually at a minimum and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.6 SUBTASK 6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted **(Section F, Deliverable 14)**. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in **Section J, Attachment G**.

C.5.1.7 SUBTASK 7 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout TO performance. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified **(Section F, Deliverable 04)**. The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

C.5.1.8 SUBTASK 8 – TRANSITION-IN

The contractor shall provide transition-in services for the TO. The contractor shall execute a two-phased transition process as outlined in **Section J, Attachment AA**. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall conclude all transition-in activities no later than 180 calendar days after TOA.

The contractor shall provide a Transition-In Plan **(Section F, Deliverable 03)** for Government approval that shall address the Tasks in Section C.5, identifying the roles and responsibilities of the contractor and any incumbent contractor(s) (if applicable), information expected from the incumbent contractor(s) (if applicable), the process to ensure that current vital USACE activities that are within scope of the TO are continued without disruption, a draft schedule(s), to include the anticipated timeline for appropriate personnel security processing, and milestones to ensure no disruption of Government service during and after the transition-in period.

The Transition-In Plan shall document how the contractor plans to seamlessly transition all existing services from the current provider(s), add new services, and minimize operational and project impacts. At a minimum, the Transition-in Plan shall include:

a. Transition schedule with tasks, duration, milestones, resource allocation, knowledge transfer sessions, and dates for completion of work transfer from current provider(s) to contractor.
b. Plan sections dedicated to the transition of Operational and Service Desk support with emphasis on integration with the outgoing provider and obtaining system access to support seamless hand-off of responsibilities.
c. Contractor onboarding plan and schedule that considers time to initiate background investigations and receive initial enter on duty determination to obtain access card, network and email account, and complete USACE-required training.
d. Summary and schedule for Government-Furnished Information (GFI), Government-Furnished Equipment (GFE), and space.
e. Schedules for Transition-In Progress Reviews (IPR), Status Reports, and Operational Readiness Review(s).
f. Risks and associated risk mitigation plans.

The contractor shall implement its Government-approved Transition-In Plan No Later Than (NLT) fifteen calendar days after the TO Kick-Off Meeting. Phase One transition activities shall be completed 90 calendar days from TOA with the contractor achieving full operational performance for the task identified in **Section J, Attachment AA**. Phase Two transition

activities shall be completed 180 calendar days after TOA with the contractor achieving full operational performance for tasks as identified in **Section J, Attachment AA** 140 calendar days after approval of the Transition-In Plan **(Section F, Deliverable 03)** but NLT 180 calendar days from TOA.

C.5.1.9 SUBTASK 9 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within six months of Project Start (PS) **(Section F, Deliverable 15)**. The contractor shall review and update the Transition-Out Plan in accordance with the specifications in **Sections E** and **F**.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Asset Inventory identifying Contractor or Government ownership.
i. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.1.10 SUBTASK 10 – SERVICE INTEGRATION AND MANAGEMENT (SIAM)

Support services will be segmented between the Government and the contractor, and other service providers. The Government requires the contractor's approach to SIAM to provide coordination of multiple service providers with the goal of seamlessly integrating interdependent services from various internal Government and external service providers into efficient, innovative, agile, and cost-effective, end-to-end services that meet USACE mission needs.

The contractor shall act as the primary service integrator for IT related services. The Government will act as the primary Service Integrator (SI) for other services and for integration, as needed, between the contractor and other service providers.

The contractor shall document all support requirements in a SIAM Plan and shall provide it to the Government (**Section F, Deliverable 05)** at the Kick-Off meeting. The SIAM Plan is an

evolutionary document that shall be updated annually at a minimum and as program changes occur. The contractor shall work from the latest Government-approved version of the Plan.

C.5.1.11 SUBTASK 11 – IMPLEMENT A TASK ORDER (TO) MANAGEMENT PORTAL

The objective of the TO management portal is to introduce efficiencies and ensure coordinated service delivery and provide a central location for the Government and contractor to access management-level information regarding the status and health of TO activities.

The contractor shall implement and maintain a secure, web-based portal capability that provides program management views/reporting, tracks metrics, and stores artifacts at the unclassified level. Government-approved contractor personnel and Government personnel shall have access to the portals worldwide. The portal shall be Common-Access Card (CAC) or Personal Identity Verification (PIV) enabled to allow users with either a CAC or PIV credential access. The portal content shall be maintained and revised throughout the duration of the TO. The contractor shall implement cybersecurity best practices to protect the portal system and data contained within the portal.

At a minimum, the portal shall provide the following:

a. Secure logical access controls with user-based views.
b. A dashboard that identifies each TDL being supported:
    1. Customer POC and entity.
    2. Lead contractor POC information.
    3. Project duration.
    4. Applicable schedule information.
    5. Allocated budget by CLIN.
    6. Funded amount by CLIN.
    7. Incurred cost amount by CLIN.
    8. Invoiced amount, invoice number and date(s).
c. A staffing roster inclusive of name, TDL, functional role, location, and clearance level.
d. An automated workflow for Government review/approval of RIPs/CTPs, TARs, deliverables, and TDLs, inclusive of the USACE TPOC and FEDSIM COR.
e. The ability to view financial information to allow the Government to track financial health. The Government will establish the level of granularity needed at the onset of an effort (funding document, ACE Work Center or line of accounting level).
f. Financial reporting capabilities to meet USACE OCIO/G-6 resource management requirements, to include Technology Business Model (TBM) and the tracking of expenses to the lowest activity level.
g. An organized document library to store management-related deliverables (e.g., monthly reports, meeting minutes, financial reports, PMP, etc.)
h. The contractor's portal solution shall provide and maintain an enterprise IT services dashboard. The dashboard shall provide automated and Government-accessible, enterprise-wide metrics, statistics, and real-time data on critical success factors and key

performance indicators regarding the provisioning of IT services to support performance management objectives and decisions on the investment and management of IT resources. The contractor shall maintain, in a readily accessible and easy-to-use format, the capability to display (report) information critical to the USACE OCIO/G-6 and customer base on an enterprise-wide basis including, but not limited to: system outages, application issues, cybersecurity information, call-center statistics, health and performance of critical IT services, and status of service desk tickets. The dashboard shall allow OCIO/G-6 to query information, generate custom reports, and conduct data fusion.

i. Risk management information, including identification of risks, severity, and extent, identification of security tool effectiveness, and risk-based prioritization of efforts.
j. Lessons learned database to assist with process improvement projects.
k. Results of assessment or audit, including pre-audit, during, and after audit assessments.
l. Telecommunications management information, including expense management.
m. Task reporting and approval capability, to track internal USACE OCIO/G-6 tasks and packets for approval and execution.

The contractor shall deliver a proposed portal solution at the TO Kick-Off Meeting **(Section F, Deliverable 07)** for approval from the FEDSIM COR. The contractor shall implement and have its portal solution fully operational by 90 calendar days after TOA. The portal capabilities are expected to evolve and adapt to meet the mission needs of the Government.

C.5.1.12 SUBTASK 12 – IT GOVERNANCE

Governance is a necessary component for ensuring effective integration of enterprise-wide IT services into the USACE environment. The contractor shall provide IT governance services to identify cost and other service management details to ensure USACE remains a leader in technology management, exceeding the expectations set forth by OMB's annual objectives, as well as providing cost transparency to the USACE OCIO/G-6 customer base. The contractor shall ensure compliance with all applicable (e.g., Federal, DoD, Army, OMB, USACE, etc.) regulations and policy during TO performance.

The contractor shall provide USACE IT Governance Documentation (**Section F, Deliverable 16)** that shall assist USACE OCIO/G-6 and USACE stakeholders, customers, and end users with strengthening and enhancing USACE OCIO/G-6's IT operating environment. Governance documentation shall be submitted to USACE OCIO/G-6 for review and approval.

The contractor shall review proposed changes to Government IT policies, architectures, standards, and procedures, and recommend additions, modifications, and deletions as needed to satisfy governance requirements. The contractor shall advise the Government of any adverse impacts to stability, cost, architecture, interoperability, compatibility, and service and recommend mitigation strategies. Governance of the IT services delivered to USACE is a significant effort requiring a joint commitment from the Government governance teams and the contractor governance teams.

C.5.1.13 SUBTASK 13 – PREPARE AND UPDATE TECHNICAL DIRECTION PLAN(S) (TDPs)

The Government anticipates that this will be a project-based TO with multiple projects operating concurrently among the USACE organizations. Work within the scope and tasks of the TO will be directed by USACE OCIO/G-6, TDL, in accordance with H.15, initiated by the Government and completed by the contractor in the form of a Technical Direction Plan (TDP). The FEDSIM CO will provide written confirmation and approval that each TDP is within the TO scope of requirements. The contractor shall provide all expertise and services as stated in the TO to deliver the integrated professional services.

TDLs will be initiated at varying times within a PoP, consisting of various appropriation types (e.g., one-year, two-year, or no-year), depending on the bona fide need.

In response to the Government's TDL, the contractor shall provide, at a minimum, the following information as part of a TDP:

a. Summary of the Government's requirements that includes, at a minimum, the project specifications, structure, activities, conditions, risks, mitigations, and schedule from project inception through project closeout. All project milestones shall be detailed with clear, unambiguous target dates.
b. Project staffing and resource profile.
c. Travel and ODC considerations.
d. Security considerations.
e. Detailed project cost estimate broken out by CLIN.

Once the TDP **(Section F, Deliverable 17)** has been approved by the FEDSIM CO and FEDSIM COR, the contractor shall schedule and coordinate a TDP Kick-Off Meeting **(Section F, Deliverable 18)** at a location approved by the Government if required. Project Kick-Off Meetings may be held virtually pending approval from the FEDSIM COR. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the project. The meeting shall provide the Government and the contractor with an opportunity to discuss technical, management, and security issues as well as other TO processes and procedures. At a minimum, the attendees shall include the contractor PM, relevant Government representatives, the USACE OCIO/G-6 TPOC, and the FEDSIM COR.

Prior to the TDP Kick-Off Meeting, the contractor shall provide a TDP Kick-Off Meeting Agenda **(Section F, Deliverable 19)** for review and approval by the FEDSIM COR and the USACE OCIO/G-6 TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics:

a. Introduction of team members and personnel including roles, responsibilities, and lines of communication between the contractor and the Government.
b. Discussion of the TDL requirements.
c. Discussion of the cost estimate.
d. Discussion of staffing and status.

The contractor shall draft and provide a TDP Kick-Off Meeting Minutes Report **(Section F, Deliverable 20)** documenting the TDP Kick-Off Meeting discussion and capturing any action items.

Following the project Kick-Off Meeting, the contractor shall provide the updated TDP **(Section F, Deliverable 17)** to the FEDSIM CO and FEDSIM COR for review and approval in accordance with Section E. The TDP is an evolutionary document that shall be updated, at a minimum, annually or as changes occur or the project reaches completion **(Section F, Deliverable 17)**. The contractor shall work from the latest Government-approved version of the TDP. In the event there is a conflict between the TDL and the TO, the TO shall always take precedence. The FEDSIM CO will approve all changes.

C.5.2 TASK 2 – ENTERPRISE SHARED SERVICES

USACE OCIO/G-6 requires infrastructure and shared services, including the day-to-day operational activities required of the contractor to provide end-to-end, enterprise-level monitoring, management, administration, performance optimization, and maintenance for all IT services, devices, applications, and infrastructure. The contractor shall support physical devices and software applications inclusive of hardware, software, networks, and facilities that are required to develop, test, deliver, monitor, control, purchase, or support IT services necessary to operate the entire enterprise. The contractor shall support USACE's current operations by performing assessments, submitting recommendations, and executing phased service implementations to migrate IT to as-a-service models or improve current state where appropriate and approved by USACE CIO **(Section F, Deliverable 21)**.

Enterprise shared services are IT services and procurements that are common among USACE operating units.

C.5.2.1 SUBTASK 1 – MANAGED SEAT SERVICES

The contractor shall provide IT services to all supported CONUS and OCONUS locations. Services shall be provided in accordance with standard approaches, such as ITIL current version, Configuration Maturity Model Integration (CMMI) for development, CMMI services, International Organization for Standardization (ISO)/International Electro technical Commission IEC 20000-1:2011, ISO/IEC 27001, or a comparable service delivery methodology. The Revolutionary Information Technology Services (RITS) contractor shall assume the current IT environment initially utilizing existing, Government-owned devices to the most practical extent, and then phase in revised solutions based on Government-approved transformations.

The contractor shall:

a. Provide zero or thin client, desktop, laptop, and high-performance end-user computing services and peripheral devices to approved USACE employees.
b. Provide remote access capability for all seat service end users in the CONUS and OCONUS.
c. Provide comprehensive customer service, including remote support, deskside support (as required), self-service, and walk-up service to ensure continued productivity of end users.

d. Provide access to customer support through a wide variety of channels including email, internet, chat, and telephone.
e. Provide identity, credential, and access management services.
f. Provide capability for handling the day-to-day logistics of deploying integrated solutions, including, but not limited to, ordering, scheduling, provisioning, imaging, patching, securing, sanitizing, testing, tracking, distribution, storage, and transportation of assets.
g. Provide onboarding solutions to allow new employees to complete USACE IT onboarding requirements efficiently.

C.5.2.2 SUBTASK 2 – PRINT SERVICES

C.5.2.2.1 BASIC PRINT SERVICES

The contractor shall provide each USACE division, basic print services for all devices identified**,** and will be required to operate, install, configure, and maintain printer devices, including printers, fax machines, copiers, scanners, postage meters, and plotters. The contractor shall maintain the device inventory. The Government will provide and install paper, toner, or ink cartridges.

C.5.2.2.2 MANAGED PRINT SERVICES

The contractor shall provide managed print services when requested by any USACE division in accordance with the TDL process specified in **Section H.15**. Managed print services are completed in lieu of basic print services, and the contractor TDL shall only identify increases in labor and cost above that required by basic print services (**Section C.5.2.2.1**). The contractor shall analyze the printing needs of the division and provide the appropriate devices in a COCO model to optimize efficiency and minimize costs. Devices include printers, fax machines, copiers, scanners, postage meters, and plotters. The contractor shall be solely responsible to ensure devices are operational at all times and shall be solely responsible for all repairs and device replacements. The contractor shall maintain the device inventory and provide paper, toner, or ink cartridges.

C.5.2.3 SUBTASK 3 – UNIFIED COMMUNICATIONS (UC) SERVICES

USACE requires UC services to integrate communication platforms and optimize the end-user experience. The contractor shall provide a best-in-class UC service, recommend improvements and enhancements to the Government, and execute successful upgrades and transitions when requested and approved by the Government. The contractor shall provide VTC, audio/visual, and telepresence support, including training, set-up, maintenance, troubleshooting, and repair. Additionally the contractor shall support, manage, and ensure operability of USACE communications systems that operate on analog or digital connectivity (Private Branch Exchange (PBX), fax machines, Public Switched Telephone Network (PSTN), Plain Old Telephone Service (POTS) lines etc.).

C.5.2.3.1 VIDEO TELECONFERENCE (VTC) SERVICES

The contractor shall provide core UC VTC services and audio/visual and telepresence support and expertise to ensure successful VTC operation by USACE end users. Required services include, but are not limited to, training end users on how to use equipment; placement, set-up, maintenance, testing, and troubleshooting of equipment; and completing repairs necessary to ensure proper operation of all equipment in conference rooms, training rooms, auditoriums, offices, workspaces, and telepresence rooms.

Any inoperable VTC equipment shall be repaired or replaced by the contractor. All facets and components of the VTC system are the responsibility of the contractor.

The contractor shall provide VTC-hosting capability to support VTC connections by multiple simultaneous participants, including conference room and desktop VTC systems containing both internal and external connections. The contractor shall configure and maintain the entire existing audio conferencing and VTC system, including the IP bridge and registered systems directory.

The Government will order via the TDL process identified in **Section H.15** on site support services as required. The contractor shall provide capability for an on-site and in-person contractor presence for live troubleshooting and support of classified (Secret) and non-classified meetings. Additionally, the contractor shall support live streaming of meetings and events when requested.

C.5.2.3.2 INTERNET PROTOCOL (IP) VOICE SERVICES

The contractor shall provide core UC IP voice services, including training end users on how to use equipment and the procurement, placement, set-up, maintenance, and compliance verification of equipment, inclusive of testing, troubleshooting, and completing repairs necessary to ensure proper operation of all IP voice equipment in conference rooms, training rooms, auditoriums, offices, workspaces, and telepresence rooms. Any inoperable IP voice equipment shall be repaired or replaced by the contractor. All facets and components of the IP voice system are the responsibility of the contractor. Additionally, the contractor shall provide support services for the installation, operation, and management of UC software that enables end users to manage IP voice service from either their computer or their IP voice equipment, and 911 location services in accordance with the DoD Policy Reference Ray Baum's Act of 2018, H.R. 4986, 115th Congress (2018), identifying the area of building and floor for emergency response providers in emergency situations.

C.5.2.4 SUBTASK 4 – INFRASTRUCTURE SUPPORT SERVICES

USACE OCIO/G-6 requires infrastructure support services to continually align enterprise IT capabilities with USACE's evolving cloud migration strategy. This shall ensure the IT service delivery can effectively support the current and future IT requirements of USACE OCIO/G-6, customers, and end users.

The contractor shall assume responsibility for the current, Government-owned, end-user environment and implement a contractor's lifecycle management plan for maintenance of OCIO/G-6 supported infrastructure. Contractor-provided services shall include managing and maintaining existing infrastructure (UNIX/LINUX/AIX/Windows Servers) and ensuring legacy

IT systems and business applications operate seamlessly with contractor-provided services, installation, configuration, maintenance, upgrades, and version currency and refresh of infrastructure and devices. Contractor-provided operations and maintenance of USACE infrastructure requires capacity for changes in technology or reconfiguration as a result of the business environment.

During TO performance the contractor shall support USACE's cloud smart migration strategy, including providing scalable, metered solutions capable of supporting USACE's application and data storage needs, to include Datacenter-as-a-Service (DCaaS), Federal Risk and Authorization Management Program (FedRAMP), and DoD Provisional Authority (PA)-authorized commercial cloud capabilities. The contractor's cloud solution shall scale compute capabilities appropriately in terms of central processing unit processing power, available memory, and available storage space, to accommodate surges in usage or data. The contractor shall ensure all DCaaS service needs are adequately provided including, but not limited to, cooling, power supply, server components, backups, Disaster Recovery (DR), bandwidth, capacity, and storage. The contractor shall support existing data center cloud and future cloud migration strategy. The contractor shall continually provide performance optimization and remediate degradation, performance analysis, baseline, monitoring, alerting, root cause analysis and remediation, and continuous improvement proposals.

C.5.2.5 SUBTASK 5 – INTERNAL AND EXTERNAL CAMPUS CONNECTIVITY

USACE is continually updating bandwidth to meet mission needs of operating divisions. As a result, service distribution methods such as switching to fiber from coaxial cable may be required. USACE requires the contractor to develop, plan, and implement innovative turnkey, connectivity solutions for campus environments, including building-to-building connectivity for non-standard locations such as hydroelectric stations, parks, locks, and dams. All designs and implementations shall be in accordance with DoD, USACE, and industry standards and best practices where DoD and USACE standards do not currently exist. Coordination with local facilities for on-site support may be required.

The contractor shall develop, plan, implement, and/or review others' plans for a structured turnkey inside-plant, cabling solution that will support wired and wireless voice, data, and video services to the desktop **(Section F, Deliverable 22)**. This solution shall support the USACE mission at all USACE sites, including, but not limited to, HQ, districts, divisions, field sites, vessels, military installations, and remote locations. The contractor shall provide these services as required and identified by local government IT personnel.

C.5.2.6 SUBTASK 6 – NETWORKING

The contractor shall provide network infrastructure services. For each of the below services, the contractor shall engage in continuous troubleshooting, evaluation, and improvement of capabilities to provide a continuously improving network environment.

The contractor shall provide and maintain a Network Operations and Security Center (NOSC) capability in accordance with DoD Instruction (DoDI) 8530.01 and Army Regulation (AR) 25-1, incorporating all facets of a Security Operations Center (SOC), and a Network Operations Center (NOC). The contractor-provided NOSC shall support network communications, including data,

voice, and video services, at USACE locations throughout the CONUS and OCONUS locations, provide continuous (24 hours per day, seven days per week, 365 days per year (24/7/365)) network performance monitoring, incident detection, network security functions, and problem resolution. The NOSC shall perform the dual roles as one entity maintaining a high degree of communication with service owners.

The contractor shall provide managed Wide Area Network (WAN), Metropolitan Area Network (MAN) and managed Local Area Network (LAN) services, encompassing access layer, distribution layer, and network core components.

C.5.2.7 SUBTASK 7 – ENTERPRISE IT SERVICE DESK

The service desk shall provide support to users of USACE's internal infrastructure, applications, systems, and devices (including end-user devices and mobile devices) utilized by USACE. The service desk shall be the single POC for USACE end users and customers for all IT areas, applications, and business processes to report incidents; submit service requests; seek advice; obtain training; request hardware, mobile devices, or software; and register complaints about USACE's IT infrastructure, devices, applications, and programs supported in the environment. The service desk shall aggressively identify root causes impacting customer experience and work to eliminate all recurring issues identified as detrimental to overall service levels. Furthermore, the service desk shall support USACE by identifying system bottlenecks and developing mitigation and action plans to correct system performance issues.

The service desk shall also provide an interface for users to access other service management functions, such as, but not limited to, requests for services, change management, problem management, configuration management, and release management. The service desk shall use a tracking solution for all incoming incidents; provide automated ticket tracking, routing, escalation and email notifications; provide basic incident and service request management; and display basic self-service options for end users. The contractor shall provide service desk support that shall support remote end users 24/7/365 and cover classified and unclassified systems.

C.5.3 TASK 3 – GENERAL IT SUPPORT

General IT support includes monitoring and maintaining USACE databases and systems, completing installs, configuring hardware and software, and solving technical problems.

C.5.3.1 SUBTASK 1 – DATABASE SUPPORT

The design, development, management, inclusive of migration and optimization, enhancement, and sustainment of data and databases in the USACE OCIO/G-6 portfolio of systems are critical to the USACE mission. The contractor shall:

a. Administer databases and related components to include incorporating changes or updates.
b. Provide continuous improvement to existing databases to include the integration of the information within the database to facilitate data sharing across the applications.
c. Adhere to current Government data standards.

C.5.3.2 SUBTASK 2 – SYSTEMS ENGINEERING

The contractor shall provide a Systems Engineering Management Plan (SEMP) **(Section F, Deliverable 23)**. In support of USACE systems engineering, the contractor shall:

a. Identify customer and stakeholder needs.
b. Capture and evaluate customer requirements.
c. Design, build, test, and deploy solutions to meet customer requirements.
d. Analyze the impact of emerging technologies on current strategies and develop a vision for the technological future of USACE.
e. Track the alignment of IT and information management trends with USACE mission requirements and influence the deployment of technology.
f. Lead activities to investigate, plan, and manage the deployment of products and services into the USACE operating environment; address IT performance gaps and technology overlaps throughout the USACE operating environment.
g. Conduct technology feasibility assessments.
h. Utilize commercially available tools to establish performance baselines, monitor systems performance against established baselines, identify performance issues, and develop and implement solutions to enhance and maximize system performance in accordance with the contractor's approved SEMP.
i. Conduct comprehensive evaluations of technology solutions and document findings in the appropriate repository of record.
j. Support the establishment and management of an enterprise engineering service brokerage model to ingest customer requests, define requirements, and prioritize, resource, schedule, and execute engineering services using standardized processes and procedures.
k. Provide expert knowledge and skill in planning and designing engineering solutions required to support systems engineering and integration efforts integrated with cyber security to meet customer requirements.
l. Produce associated documentation requirements, templates for deliverable artifacts, forms, and checklists.

C.5.3.3 SUBTASK 3 – WEBSITE DEVELOPMENT

The contractor shall support USACE personnel with website development that accurately reflects USACE messaging and promotes the strategic objectives of USACE communications. The contractor shall ensure that all public-facing websites and content are in compliance with USACE's Public Affairs (PA) website standards to ensure a consistent appearance and style. The contractor shall support activities to ensure the registration and vulnerability assessments of websites are performed prior to promotion and lifecycle management has been engaged for the site.

C.5.3.4 SUBTASK 4 – END-USER TRAINING

In conjunction with the administration, development, release, or replacement of enterprise-level initiatives, the contractor shall assess end user training needs, develop a Training Plan (**Section**

F, Deliverable 24) and deliver training required for end users. The contractor shall maintain repositories of training documentation in formats widely accessible to stakeholders. The contractor shall provide a solution for end users to provide feedback on training taken in order to continually monitor and improve subsequent trainings.

C.5.3.5 SUBTASK 5 – ARCHITECTURE SUPPORT SERVICES

USACE OCIO/G-6 requires infrastructure architecture support services to align USACE enterprise capabilities to the vision and direction of the overall USACE Enterprise Architecture (EA) effort. This shall ensure that USACE OCIO/G-6 service delivery can effectively support the current and future IT requirements of USACE end users and clients.

EA is systematically derived and captured descriptions depicted in models, diagrams, and narratives specifically using the current DoD Architecture Framework (DoDAF) views that shall be developed in industry standard tools (USACE currently support MagicDraw tool) and in technical terms (such as hardware, software, data, communications, security attributes, and performance standards). It provides these perspectives for the enterprise's current environment and for its target environment, and it provides a transition plan for moving from the current to the target environment. The contractor shall:

a. Adhere to Engineering Regulation (ER) 25-1-112 Information Technology Architecture or successor documents.
b. Develop, maintain, and update technical documentation describing the current EA and changes to Technical Baselines and Integrated Architecture Products **(Section F, Deliverable 25)** for EA modifications in design/planning phase and/or post-implementation.
c. Perform annual configuration audits to validate configuration items are accurately represented in the USACE Technical Baselines, Integrated Architecture Products, and design and installation documentation **(Section F, Deliverable 26)**.
d. Identify and keep a current comprehensive list of USACE data structures, sources, categorizations, and formats.
e. Create or update design documentation to support all changes, new services, and technology refresh installations **(Section F, Deliverable 27)**.
f. Propose, design, and document location modifications to connect MAN or LAN to local Service Delivery Point (SDP) in accordance with location WAN circuit mapping.
g. Deliver all design hardware and software specifications and Bill of Materials (BOM), including incorporation of input from the Government **(Section F, Deliverable 28)**.
h. Assess, validate, and update the mapping to USACE OCIO/G-6 systems in the USACE OCIO/G-6 product baseline. The update shall include the delineation of segment services.
i. Provide as-built and network topology drawings **(Section F, Deliverable 29)**:

C.5.3.6 SUBTASK 6 – ENGINEERING DESIGN SUPPORT SERVICES

The contractor shall provide Engineering Design Support Services (EDSS) that encompass the engineering and technical support services required to design, model, test, pilot, and implement the systems and infrastructure required to deliver IT projects including, but not limited to, voice,

video, and data services, at the enterprise and local site levels. EDSS shall provide the Government with advice, assistance, investigation, coordination, and implementation services for improvement or addition to existing solutions or implementation of emerging solutions. EDSS shall incorporate cybersecurity requirements to ensure developed systems meet all cybersecurity requirements

C.5.3.7 SUBTASK 7 – SOFTWARE DEVELOPMENT SERVICES

The contractor shall establish a software engineering capability, available only when requested, that rapidly delivers secure and working products and software solutions. All source code developed and utilized by the contractor in performance of this subtask shall be provided to the Government, **(Section F, Deliverable 30)**. The contractor's software engineering capability shall apply all relevant fields of engineering to include physical systems, requirements, design, development, testing, deployment, maintenance, and modernization of software systems.

The contractor shall establish software development lifecycle and engineering processes based on commercial best practices. In implementing this process, the contractor shall establish a DevSecOps pipeline that builds in security and maximizes the concept of Continuous Integration (CI)/Continuous Delivery (CD) that automates build, integration, and test processes. The software engineering capability shall enable an iterative approach to design, development, testing, and implementation. The contractor shall provide software registration portals to track owner, developer, and requirements of produced software. The contractor shall provide results from software testing and requests needed for application whitelisting.

C.5.3.8 SUBTASK 8 – ASSET AND CONFIGURATION MANAGEMENT

The contractor shall provide asset management in accordance with ITIL best practices and DoD, Army, and USACE guidance. The contractor shall provide an Asset Management Plan **(Section F, Deliverable 31)**. The contractor's Asset Management Plan shall include a complete solution to document and track USACE OCIO/G-6's hardware and software assets. The contractor shall perform lifecycle management, including reporting and maintaining version currency, vendor/manufacturer maintenance, property receipt, refresh, inventory control, equipment staging and distribution, warranty repair coordination, erasure and cleansing, and transfer or destruction of hardware assets.

The contractor shall provide configuration management based on ITIL, USACE and industry best practices. The configuration management solution **(Section F, Deliverable 32)** shall be capable of capturing and maintaining the varying attributes and relationships of the Configuration Items (CIs) necessary for IT service delivery and modeling proposed changes for impact analysis. The Configuration Management Database (CMDB) for OCIO/G-6 is the tool and database used to manage and model configuration data for OCIO/G-6 infrastructure assets from design to retirement. The CMDB tool collects, stores, manages, updates, and presents data about all CIs, including the relationships between CIs and services.

C.5.3.9 SUBTASK 9 – SOFTWARE LICENSE AND HARDWARE MAINTENANCE AGREEMENT MANAGEMENT

In coordination with USACE OCIO/G-6, the contractor shall develop and provide License and Agreement Management and Tracking Procedures **(Section F, Deliverable 33)** for each USACE CIO G/6 software license and/or maintenance agreement. When directed by the Government, the contractor shall purchase license and maintenance agreements for use by the USACE OCIO/G-6 users. The contractor shall ensure licenses and agreements are purchased in accordance with current OMB, DoD, and USACE policies. The contractor shall ensure that all software license transfers (e.g., the transfer of licenses during a device refresh and/or the transfer of licenses during resource attrition) are reflected in the applicable asset management system. Additionally, the contractor shall maintain the USACE OCIO/G-6 software library. The contractor shall maintain the USACE OCIO/G-6's centralized software library to ensure that media exists for each software asset; proof of entitlement and software restrictions or usage rights exists for each software asset; proof of maintenance exists for each software asset; media installation or other security codes to install software assets exists for each software asset; and all records and media are duplicated in an offsite location for DR purposes. The contractor shall develop and implement a process for individual users to request software, evaluate the request, provide recommendations for acceptance, and purchase and deploy software. Additionally, the contractor shall identify, document, and report license compliance issues by end users and recommend solutions to resolve issues. The contractor shall provide software license usage identifying additional licenses when appropriate and also making recommendations for removal. As USACE OCIO/G-6 continues its migration to a Software-as-a-Service model (SaaS), the contractor shall provide support, including the management of enterprise licensing, identification of possible SaaS offerings that will benefit USACE, and implementation of SaaS solutions.

C.5.3.10 SUBTASK 10 – SHAREPOINT DEVELOPMENT AND ADMINISTRATION

The contractor shall provide SharePoint development and administration support to all USACE OCIO/G-6-supported organizations utilizing SharePoint sites.

C.5.4 TASK 4 – CYBERSECURITY

USACE, as an Organizational Network (ORGNET) Cyber Security Services Provider (CSSP) aligned under Army Cyber Command (ARCYBER), executes the cybersecurity activities and functions to direct the security, operations, and defense of the USACE-controlled portion of the Defense of Defense Information Network (DoDIN), consistent with all orders, regulations, policies, memorandums and/or directives to counter cyberspace threats and mitigate vulnerabilities. USACE OCIO/G-6 Cyber Security conducts the cybersecurity functions of identify, protect, detect, respond and recover within the CorpsNet infrastructure, USACE Enterprise SIPRNet, cloud environments owned or operated on behalf of USACE, CorpsNet connected SCADA and OT systems connected to CorpsNet, and the USACE agency-level instances of Joint Regional Security Stack (JRSS). USACE cybersecurity activities and functions ensure the availability, integrity, and confidentiality of the information and information systems used by USACE commands and mission areas. USACE OCIO/G-6 Defensive Cyber Operations (DCO) provides services for the protection, monitoring, analysis, detection, and response to unauthorized activity. DCO services are required to defend against unauthorized activity on all

supported networks, to include, but not limited to, activities from advanced persistent threat actors, external hackers, insider threats, and all others who may attempt to gain unauthorized access.

The contractor shall provide cybersecurity services for USACE in accordance with all Federal, DoD, Army, and USACE-specific security initiatives. The contractor's cybersecurity services shall be proactive, continuous, and result in "inspection ready" systems and environments at all times, and shall be postured to achieve passing scores on all inspections, to include, but not limited to, no notice Command Cyber Readiness Inspections (CCRIs). The contractor shall implement all phases and aspects of DoD accreditation/certification policies and procedures for the USACE-controlled portion of the DoDIN during the entire lifecycle for all USACE systems and environments. The contractor shall provide consistent and complete documentation that satisfies all policy and reporting requirements TO ESTABLISH the USACE Reporting and Analysis Program, which reports to appropriate Federal, DoD, Army, and USACE organizational entities, such as the OMB, DoD Inspector General, DISA, Army Network Enterprise Technology Command (NETCOM), ARCYBER, Army CIO/G-6, and USACE OCIO/G-6 and Command staff.

The contractor shall develop a Cybersecurity Strategy Plan (CSP) **(Section F, Deliverable 34)**, that describes concisely how a program's cybersecurity features comply with applicable standards, regulations, and requirements. The CSP shall identify how the contractor shall meet the following subtasks.

C.5.4.1 SUBTASK 1 – PATCHING AND VULNERABILITY MANAGEMENT

The contractor shall implement, configure, operate, and maintain an automated patch and vulnerability management capability to maintain compliance for assets and technologies within the USACE controlled portion of the DODIN. In support of patching and vulnerability management, the Contractor shall:

a. Maintain current anti-malware, software, engines, and signatures, vendor patches, IAVM, in accordance with DoD, Army, and USACE OCIO/G-6 directives, policies, and procedures
b. Minimize the impact of patching and scanning on USACE operations and end users.
c. Maintain proactive awareness of changes in the threat landscape and/or vulnerabilities and propose and execute mediatory actions.
d. Implement a process for emergency vulnerability notifications for accelerated timelines.
e. Comply with DoD, Army, and USACE OCIO/G-6 reporting requirements.
f. Conduct and analyze STIG, IAVM, and non-IAVM scans. Address and mitigate non-compliant devices or configurations, adhering to the organizational change management process **(Section F, Deliverable 35)**.
g. Conduct vulnerability tests within a test environment to identify operational impact of activity directed against USACE systems or applications to identify USACE-wide impacts as requested.
h. Provide a Plan of Actions and Milestones (POA&M), Operational Impact Statements (OIS), or Waiver if STIG(s) or IAVMs cannot be achieved, providing

mitigation/remediation strategies to reduce risk to achieve STIG compliance **(Section F, Deliverable 36)**.

i. Schedule, assign, and monitor POA&M action items until completion by or before the established suspense date.
j. Report status of STIGs or IAVMs for all applicable technologies, assets, etc. **(Section F, Deliverable 37)**.
k. Ensure no un-remediated AVMs exist on the network without an approved POA&M or Waiver or one that has been preceded with a later IAVM version.
l. Ensure correlation of STIG and IAVM-required audit and accountability transaction alerts are fed into Security Information and Event Management (SIEM).

C.5.4.2 SUBTASK 2 – STRATEGY, POLICY, AND CONTINUOUS IMPROVEMENT

The contractor shall analyze the current USACE OCIO/G-6 security strategy, posture, policies, and operations to identify areas for improvement **(Section F, Deliverable 38)**. Improvements may be based on best practices or new technologies and shall be appropriate for all environments and missions. The contractor shall support continuous improvement and shall:

a. Review, assess, and recommend mitigation actions on new vulnerabilities (e.g., zero-day etc.).
b. Enhance performance of asset data collection and maintenance.
c. Collect and analyze lessons learned for potential process improvements and incorporate applicable lessons learned into current policies, guidelines, checklists, procedures, and/or other appropriate means. All lessons learned shall be documented and maintained in the contractor's TO portal.
d. Provide budget and fiscal support which includes, but is not limited to, analysis and documentation of budgetary information as it relates to meeting requirements, risk discussion, return on investment, value, and outcome.

C.5.4.3 SUBTASK 3 – MANAGED SECURITY SERVICES (MSS)

USACE OCIO/G-6 requires MSS to safeguard USACE-supported networks and systems against ever-evolving security threats. MSS provide protection of endpoints, email, web, and networks, and include capabilities such as authentication, antivirus, anti-malware/spyware, intrusion detection, and incident response. The contractor shall provide up-to-date situational awareness of network security services, devices, and resources associated with MSS, including, but not limited to, Application Filtering (Layer 7), Network Time Protocol (NTP), Domain Name Service (DNS) protocol including Domain Name System Security Extensions (DNSSEC), external registration and management, malware domain prevention/detection, malware inspection and prevention, behavior-based intrusion detection and analysis, rogue wireless access point detection and prevention, deep packet inspection and analysis, source and destination address filters, including automated Access Control List (ACL) review and policy compliance, Transmission Control Protocol (TCP) stream data capture with access to archival information for forensics purposes, Reverse Web Proxy (RWP), and secure channel inspection, analysis, and prevention.

MSS is further broken out into:

a. Monitoring services
b. Vulnerability Scanning Services (VSS)
c. Incident response services (INRS)

While identified here as separate activities, the contractor shall provide services in a holistic manner, with each individual service supporting and reinforcing the other to provide a complete MSS.

Monitoring services provides the ability to monitor hosts and network traffic, and analyze network protocol and application activity to identify and mitigate suspicious activity. This service will be provided 24/7/365.

VSS searches for security weaknesses, flaws, and open exploit vectors on the USACE OCIO/G-6 systems, networks, and applications. VSS can also simulate a real intrusion in a controlled environment, to gauge a network's susceptibility to attacks. This service will be provided 24/7/365. The service performs controlled internal and external scanning by remotely probing a network for penetration weaknesses that generally come from the outside, and internal scans that detect flaws originating from the inside.

INRS, in accordance with the Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01B Cyber Incident Handling Program, involves telephone, web, and on-site support for monitoring and analyzing alert information, and responding to malicious events such as Denial of Services (DOS) attacks; virus, worm, and Trojan horse infections; and illegal inside activities, espionage, and compromise of sensitive internal agency databases. This service shall be provided 24/7/365. INRS shall provide support through all phases of incident response (preparation, identification, containment, eradication, and remediation). INRS shall provide an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks.

MSS shall connect to and interoperate with the agency networking environments, including cloud, DMZs and secure LANs, as required by the USACE OCIO/G-6. The service shall also support connectivity to extranets and the internet.

Monitoring services shall include, but are not limited to:

a. Providing analysis and monitoring for all systems and environments to ensure the availability, integrity, and confidentiality of the data processed, stored, and transmitted via a centralized support monitoring service. Analysis and monitoring shall be automated to the maximum extent possible.
b. Providing Intrusion Detection System/Intrusion Prevention System (IDS/IPS) support:
    i. Implementing, administering, and maintaining threat sensors based on current threat directives and recommendations.
    ii. Developing, testing, and distributing threat sensor baseline signatures.
    iii. Developing IDS/IPS test plans, operational procedures, and maintenance plans **(Section F, Deliverable 39)**.
    iv. Providing host-based intrusion detection monitoring and prevention on all devices, including those supporting Host-Based Security Systems (HBSSs).

v. Providing data feeds from all intrusion detection and prevention modules for incorporation into the Enterprise Security Incident Management System, for CorpsNet, cloud, DMZ, and SIPR in accordance with classification guidance.

c. Providing continuous monitoring of malware protection and detection mechanisms.
d. Providing administrator access to the designated Government POCs as required.
e. Providing active monitoring of the operational status, health, and performance of the monitoring tools and devices.
f. Actively monitoring vendor feeds, Army feeds, tippers, OPORDS, sensor grids, and intelligence feeds for new signature information.
g. Analyzing the information provided and providing recommendations for inclusion into the CorpsNet, and SIPRNet environments, while maintaining the classification of information.
h. Providing performance measurements, logs, and information feeds from the security monitoring systems (e.g., HBSS and IPS).
i. Maintaining access to current network architecture diagrams per DISA standards showing placement of sensors (e.g., IDS/IPS, Routers, Netflow/PCAP systems, firewall, etc.).
j. Reporting on access to assets, including, but not limited to, network and host-based sensors for CorpsNet, CorpsNet extended network (JRSS and cloud), and SIPRNet **(Section F, Deliverable 40**).
k. Integrating and correlating data from USACE systems, servers, services, SIEM, and end points to measure, monitor, remediate, and remove threats to the environment in accordance with USACE OCIO/G-6 directives.

VSS shall include, but are not limited to:

a. Performing monthly wireless scanning to monitor for non-approved or rogue wireless access points.
b. Developing and maintaining scan zones for out of compliance conditions based on USACE OCIO/G-6 directives. As required, conduct ad hoc scans. Scans can be full system, specific workstation, or server scans. The contractor shall analyze scan results and provide a Recommendations Report **(Section F, Deliverable 41).**
c. Providing vulnerability testing in accordance with DoD, Army, and USACE OCIO/G-6 directives and guidance and established best business practice regulations, policies, and procedures.
d. Identifying existing defensive weaknesses or vulnerabilities. Providing assessment to USACE OCIO/G-6 to determine the best method of mitigation or continued monitoring **(Section F, Deliverable 42)**.

INRS shall include, but are not limited to:

a. Responding to alerts and violations identified, in accordance with cyber policy and incident response plans, as part of the SIEM.
b. Identifying incident threat level and nature based on the received alert or violation.
c. Identifying root cause, source, and methodology used to properly categorize the incident.
d. Providing AR 380-53 Network Damage Assessment, if necessary.

e. Gathering host logs from compromised system(s).
f. Taking corrective action to contain the incident, prevent further spread, and protect systems.
g. Providing forensically sound evidence collection and capabilities.
h. Eradicating the malicious event from infected hosts/network as directed by USACE OCIO/G-6.
i. Providing cyber clean-up as required, including the restoration of damaged data.
j. Recommending mitigating actions to prevent future infections or reinfection.
k. Configuring and fine-tuning detection/prevention capabilities.
l. Providing cyber After Action Reports (AARs), including lessons learned and final network damage assessment as identified by USACE OCIO/G-6 **(Section F, Deliverable 43)**.
m. Providing analysis, correlation, and trending of anomalous events and incidents.
n. Supporting incident response team deployment to USACE OCIO/G-6 locations.
o. Coordinating and sharing data with other Federal agencies and DoD commands as directed by USACE OCIO/G-6.
p. Providing analysis and reverse engineering of cyber threats.
q. Implementing mitigation measures in response to general or specific threats on the respective networks in accordance with USACE OCIO/G-6 directives.

C.5.4.4 SUBTASK 4 – SECURITY INFORMATION AND EVENT MANAGEMENT SUPPORT

The contractor shall implement, configure, monitor and maintain a DoD-approved enterprise SIEM tool to monitor, detect, and respond to threats on all USACE-supported networks and enclaves. The SIEM shall provide real-time analysis of security alerts generated by applications and network sensors, hardware, cyber tools, Government-approved threat intelligence feeds and threat detectors, and be capable of automatically forwarding incidents and events to the incident response team and USACE OCIO/G-6 based on severity level. The SIEM shall be configured to support classification level of data. Additional support for the SIEM shall include, but is not limited to:

a. Automated incident response capabilities.
b. Performing data correlation and analysis reporting for all sensors and defense capabilities at an enterprise level.
c. Providing the Government access to the SIEM systems, including the functionality to establish use cases and run queries.
d. Providing immediate notification for unplanned sensor-fed outages exceeding 24 hours, and providing an AAR identifying root causes for the outage **(Section F, Deliverable 44)**.
e. Maintaining documentation for all feeds, sensors, and connectors in the SIEM and providing reports to USACE OCIO/G-6 **(Section F, Deliverable 45)**.

C.5.4.5 SUBTASK 5 – CONTINUITY OF OPERATIONS (COOP) AND DISASTER RECOVERY (DR) SERVICES

The contractor shall provide IT support to USACE OCIO/G-6 COOP and DR efforts and site(s). The contractor shall develop and execute a COOP/DR Plan **(Section F, Deliverable 46)**, as directed by the Government, for USACE OCIO/G-6 COOP and DR capabilities. This plan will be exercised periodically to ensure that safeguards, backups, end-user services, and procedures can provide continuity of mission support services through issues such as natural disasters, power outages, and building loss, and allow for successful recovery of all services after facility restoration or the establishment of an alternate facility.

The contractor shall provide the following COOP-related services as directed by the Government:

a. Provide IT-related technical input to USACE OCIO/G-6 COOP planning, design, and implementation efforts, including meeting and briefing support.
b. Provide IT-related technical liaison, coordination, and Tier I/II support with COOP facility service providers.
c. Ensure USACE OCIO/G-6 systems remain viable in the event of system failover.
d. Perform scheduled COOP exercises to ensure functional and operational processes are current to infrastructure changes and are held annually at a minimum.

The contractor shall provide the following DR-related services as directed by the Government:

a. Provide technical support to DR meetings.
b. Support technical assessment and perform site surveys for DR candidate sites and hosting services in support of Government planning activities.
c. Assist USACE OCIO/G-6 in developing and documenting DR capabilities.
d. Support and administer network connectivity, cryptography, circuits, and other communications systems between USACE OCIO/G-6 and DR facilities.
e. Provide IT-related technical support to the operation of USACE OCIO/G-6 DR capabilities.
f. Support implementation, configuration, and administration of DR systems
g. Perform scheduled DR exercise to ensure the DR Plan and documentation remains up to date and current.

C.5.4.6 SUBTASK 6 – CYBER TOOLS SUPPORT

The contractor shall propose, develop, install, manage, maintain, integrate and configure a suite of cybersecurity tools to support USACE CIO G-6 network cybersecurity posture. Cybersecurity tools include, but are not limited to, hardware and software throughout CorpsNet, CorpsNet Extended Networks (CEN), network exit points, and endpoint devices performing detection, protection, prevention, analysis, response, and remediation of cyber security threats. Support shall include, but not be limited to:

a. Developing software enhancements for cyber tools and re-utilization of code, in accordance with USACE CIO G/6 priorities.

b. Developing supporting documents and maintenance schedules **(Section F, Deliverable 47)**.
c. Ensuring repositories for cyber tool backups, cyber tool configurations, scan repositories, and analysis portals are created, maintained, and available.
d. Testing and verifying for reliability backups, configuration changes, and updates.
e. Providing analysis of all monitoring tools, including, but not limited to, audit logs, IDS/IPS logs, firewall logs, audit logs, access logs, and full packet capture data for covert or malicious activity.

C.5.4.7 SUBTASK 7 – THREAT INTELLIGENCE SERVICES

The contractor shall provide cybersecurity intelligence support to identify emerging threats to the USACE OCIO/G-6 environment. The contractor shall provide the following support:

a. Develop and report tailored, all-source analysis to provide situational awareness of critical elements of the cyber environment necessary to defend the USACE and USACE extended networks **(Section F, Deliverable 48)**.
b. Maintain awareness of current activity trends on Army, other Government, and commercial networks.
c. Contribute to the body of knowledge on bad actors or adversaries' cyber capabilities and intentions.
d. Develop a priority list of high-profile personnel and groups to track. This list should include all named activities as well as other people/groups of interest.
e. Analyze the origins, pathways, and methodologies of malicious cyber activities to attribute, model, and predict future intrusions.
f. Analyze computer network intrusion events and malicious activity to support intrusion detection and cyber-attack warning and response.
g. Provide forensic analysis of captured packets, hard drive images, system logs, and sensor data used in all-source intelligence products.
h. Perform Requirements Management (RM) to track intelligence requirements and production efforts. Maintain record of all relevant cyberspace operations reports and task assignments for tracking purposes.
i. Update, maintain, and ensure quality control of appropriate classified databases and repositories.
j. Maintain liaisons and conduct technical exchanges with parent agencies and vetted partners' higher agencies. Identify exchange opportunities and conduct exchanges (formal and informal) as appropriate.

C.5.4.8 SUBTASK 8 – SECURITY CONFIGURATION MANAGEMENT (SCM)

SCM provides an enterprise-wide security compliance capability , 24/7/365, that scans and remediates USACE OCIO/G-6 IT assets, services, and all end points for out of compliance conditions such as changed settings, outdated patches, and un-approved software IAW CJCSM 6510.01B and DoD, Army, and USACE directives, policies, and procedures. The contractor shall

collaborate with the Government and other service providers to provide the services. In support of SCM, the contractor shall provide the following, including, but not limited to:

a. Providing central administration of overall USACE OCIO/G-6-related network SCM status, in combination with the Government.
b. Providing SCM scanning, data collection, and analysis.
c. Remediating and mitigating assigned SCM configurations in accordance with USACE OCIO/G-6 response processes.
d. Executing end-to-end data correlation.
e. Documenting configuration parameters.
f. Maintaining the current SCM tools and databases.
g. Identifying compliance capability gaps and recommending SCM tool optimizations to enhance performance and/or reduce user impact.
h. Reporting the availability, capacity, and performance of the security infrastructure and services.
i. Supporting authorized third-party evaluators performing vulnerability evaluations.
j. Updating SCM tools and database signature files as required.
k. Managing, maintaining, and documenting the configuration and operability of the cyber tools, databases, and logs.
l. Maintaining security configuration of cyber network defense devices.
m. Providing quarterly analysis of SCM transport services, systems, and networks to identify potential security weaknesses and exposures to known threats.
n. Providing Enterprise DAT Versioning and enterprise virus scanning software versioning reporting as required **(Section F, Deliverable 49)**.

C.5.4.9 SUBTASK 9 – DEMILITARIZED ZONE (DMZ) SERVICES

A DMZ is a logical and physical framework that allows protected access to resources from internal and external networks. Extended-DMZ (e-DMZ) or DMZ extension is a combination of hardware and software that creates a logical addition from a different physical facility to 1) the DMZ resources; or 2) a single zone in the e-DMZ.

The contractor shall:

a. Implement and maintain the DMZ infrastructure in accordance with applicable directives, policies, and OPORDs.
b. Provide DMZ configuration documentation and store appropriately.
c. Apply applicable cybersecurity and cyber change management policies when requesting and making changes.
d. Provide biannual verification and analysis of DMZ configurations and any recommendations for improvement.
e. Maintain a Bogon list and ensure implementation of Bogon updates and filters is performed within 24 hours, unless emergency conditions require a more immediate deployment..

f. Verify and monitor enforcement of public-facing web server security configurations, RWP, web content and filtering policy, and firewall action requests. Perform an annual review and analysis of each public web server, RWP policies, and Web Content Filter (WCF) rules. Generate an annual report that reviews, analyzes, and provides recommendations for each of the DMZ web servers, RWP, and WCF. **(Section F, Deliverable 50)**
g. Review new web deployments, policies, and rules; document findings and create actions to correct security issues; and provide notification to proper organizations for follow up.

C.5.4.10 SUBTASK 10 – PENETRATION TESTING (PEN-TESTING)

USACE's cyber security program is periodically required to provide results of penetration testing (pen-testing) of USACE networks and systems to validate the success of implemented security controls. The contractor shall support pen-testing of USACE networks.in coordination with the Government. The contractor shall:

a. Support pre-pen testing efforts:
    1. Provide device and system availability for testing.
    2. Provide network drawings/design documentation in accordance with classification requirements and policies.
    3. Provide internal and external network configurations required to perform pen-testing.
b. Support pen-testing activities:
    1. Escort pen-test and Red Team personnel during on-site activities.
    2. Support pen-test exercises as directed by the Government.
    3. Provide a liaison between on-site pen-test and Red Team and Government personnel, documenting activities, findings, incidents, and weaknesses.
c. Support post-pen testing and Red Team efforts:
    1. Provide analysis of pen-testing results, including a summary of security weaknesses, risks to CorpsNet and SIPRNet, and recommendations to secure the weaknesses identified **(Section F, Deliverable 51)**.
    2. Implement approved security recommendation in accordance with USACE OCIO/G-6 directives.

C.5.4.11 SUBTASK 11 – PORTS, PROTOCOLS AND SERVICES MANAGEMENT (PPSM)

The Ports, Protocols, and Services Management (PPSM) program requires USACE OCIO/G-6 under DISA, to register and carefully manage all DoD Information Systems and whitelist registrations, including the use of network Ports, Protocols, and Services (PPS). USACE OCIO/G-6 utilizes DISA's Category Assurance List (CAL) when preparing USACE projects for development and acquisition. The contractor shall support the PPSM program by:

a. Ensuring that all DoD information systems PPS that are accessible to the managed networks are acquired, developed, implemented, and registered in the PPSM central registry.

b. Using and protecting PPS according to the most current vulnerability assessment reports, and implementing them as described in the most current version of DoD STIGs on network infrastructure and application security and development.
c. Implementing and enforcing PPSM policies and procedures at the enclave boundaries, and restricting boundary firewalls and firewall-like devices to the use of approved PPS in accordance with DoDI 8551.01 or successor documents.
d. Reviewing software, hardware, and PPS against the Approved Products List, evaluated product list, and DISA CAL.
e. Conducting auditing, in accordance with the approved test plan, to verify that the designated site complies with DoD, Army, and USACE OCIO/G-6 policy.
f. Performing blocking/denying access by hostile sites or restricting access by specific ports/protocols and/or applications in accordance with USACE OCIO/G-6 policies.
g. Coordinating with DoDIN, DISA, and Army network staff as required for network configuration modifications (e.g., IP blocks/un-blocks and Uniform Resource Locator (URL)/domain blocking/unblocking) in accordance with cyber change management processes.
h. Providing PPSM management in support of changes to network and service requirements (e.g., workload migrations to cloud hosting, etc.).

C.5.4.12 SUBTASK 12 – RISK MANAGEMENT FRAMEWORK (RMF) SUPPORT

The contractor shall provide cybersecurity authorization and compliance services supporting the RMF for USACE in accordance with DoD, Army, and USACE OCIO/G-6 policies and procedures.

The contractor shall provide technical support in collaboration with USACE cybersecurity groups and technical teams to provide RMF support through the six steps of the RMF process. The contractor shall support USACE in the development of security plans, generation of assessment reports, and formulation of a remediation POA&M. The contractor shall perform the following tasks:

a. Categorize agency information systems
b. Select security controls
c. Implement security controls
    1. Produce and provide security control artifacts required by DISA for interim authority to connect and authority to connect **(Section F, Deliverable 52)**.
d. Assess security controls:
e. Authorize information systems and provide Information System Security Manager (ISSM) services
f. Monitor security state
    1. Capture, assess, maintain, and report asset information and provide an assessment report, identifying issues related to capturing of data and/or storage of data **(Section F, Deliverable 53)**.

C.5.4.13 SUBTASK 13 – FILE REMOVAL SERVICES

File removal services provide isolation and resolution when electronic spillage has occurred where classified or controlled unclassified (such as Personally Identifiable Information (PII)) information has been introduced on an IT system, network, or component that is not authorized to hold or process such information. A spillage can be from a higher level classification to a lower one. The data itself may be residual (hidden) data or metadata.

The contractor shall provide support for both classified and PII spillage

a. For classified spillage:
    1. Notify the activity in accordance with DoD, Army, or USACE OCIO/G-6 policies when there are incidents involving possible or actual compromise or data spills of classified information resident in information systems, as required.
    2. Quarantine known electronic spillage locations in accordance with cyber security directives and USACE policies.
    3. Remove all instances of the electronic spillage from the network, back-up systems, email, mobile devices, printers, and media in accordance with cyber security directives and USACE policies. Spillage locations that cannot be electronically removed shall be coordinated with designated personnel to remove and verify the electronic spillage.
    4. Start the trace process to determine the extent of the electronic spillage proliferation across systems.
    5. Provide spillage reporting as required, including, but not limited to, trace reporting, the last known locations of files that may have been further distributed but cannot be traced to service-level NOCs, and unauthorized or inadvertent disclosure summary data and results **(Section F, Deliverable 54)**.
    6. Submit a POA&M for actions that cannot be completed within timeframes required by USACE policy **(Section F, Deliverable 55)**.
    7. Notify the designated Government authority upon completion of electronic spillage cleanup.
b. For PII spillage
    1. Follow incident reporting procedure as outlined in USACE-IT PII SOP upon notification of a PII breach by the customer.
    2. Report PII to the U.S. Computer Emergency Readiness Team (US-CERT) and immediately upon notification of an incident; annotate the helpdesk ticket with the US-CERT incident number.
    3. Send PII notifications to the USACE Privacy Officer as well as to other distribution groups as defined in the USACE-IT PII SOP.

C.5.4.14 SUBTASK 14 – CYBER FORENSICS AND MALWARE ANALYSIS (CF&MA)

The CF&MA mission supports the USACE in the areas of file data collection, volatile data collection, analysis of system anomalies, malware reverse engineering, and creation of Indicators of Compromise (IOC) to improve the protection of USACE information. The USACE CF&MA

works in concert with the Army Cyberspace Operations and Integration Center (ACOIC) and ARCYBER to ensure electronic evidence collection and integrity are maintained throughout the lifecycle of the evidence.

The contractor shall:

a. Perform forensically sound electronic data collections, analysis and reverse engineering of malware, suspect code, email, malformed program objects, and volatile memory in accordance with USACE OCIO/G-6 directives, and chain of custody guides utilizing industry best practices.
b. Analyze the attack/exploit capability of malware as directed by USACE OCIO/G-6.
c. Provide all pertinent findings and IOCs to teams responsible for the development of signatures to detect the malware as it propagates on infected systems.
d. Collect, preserve, and transfer forensic evidence of unauthorized access to CorpsNet devices or information systems in accordance with USACE OCIO/G-6 policy and processes.
e. Produce analysis reports for each incident and provide them to USACE OCIO/G-6.
f. Work and interact with professionals, internal and external to USACE, to understand higher-level adversary capability.
g. Document, update, and enhance processes and procedures by producing training materials, tools, tactics, techniques, procedures, SOPs, lessons learned, and reports.

C.5.4.15 SUBTASK 15 – CYBER PLANS AND EXERCISE SUPPORT

The contractor shall support USACE OCIO/G-6 cyber plans and exercises to assess, evaluate, and update the USACE OCIO/G-6 cyber posture.

a. Administer the development, planning, and exercises to be performed.
b. Attend exercise planning conferences, provide expert advice for development of planning documentation, participate during exercise and other security cooperation events, and prepare AARs and lessons learned during all phases of DCO support exercises.
c. Support mission planning, mission analysis, technical analysis, and Concept of Operations (CONOPs).
d. Develop and/or provide input to OPORDs, CONOPs, and courses of action.
e. Support management and planning operations by submitting mission requests, providing status reports, and submitting AAR comments

C.5.4.16 SUBTASK 16 – INSPECTION AND AUDIT SUPPORT

USACE OCIO/G-6-supported environments are subjected to a variety of inspections, audits, and external reviews, including, but not limited to, the Command Cyber Readiness Inspection (CCRI), FISMA, TMF, Security Control Assessor-Validator (SCA-V), Army Protection Program Assessment (APPA), DoD Inspector General (IG), Chief Financial Officer (CFO) audits, and CSSP reviews. The contractor shall strive to conduct all cybersecurity support to provide an always audit-ready solution. The contractor shall:

a. Ensure notification and tracking of significant incidents that meet CCRI criteria.

b. Prepare and maintain network address declarations in accordance with DISA requirements. Changes shall be submitted to the USACE OCIO/G-6 for approval.
c. Provide support for inspections, audits, and external reviews, including pre- and post-audit support.
d. Provide audit readiness assessments. Assessments include, but are not limited to:
    1. Review of documentation for accuracy.
    2. Provide status of STIG, vulnerability, misconfigurations, etc.
    3. Provide Category (CAT) I, II or III remediation statistics.
    4. Estimate CCRI Scoring based on JFHQ-DoDIN CCRI Scoring, CCRI Phase IV Grading Criteria Worksheet, and CCRI Risk Indicator Scoring.
    5. Identify key issues affecting the defense of the USACE networks and cyber posture.
e. Identify systemic causes of any assessment finding, pre-audit and post-audit, and develop recommended courses of corrective actions.
f. Develop and disseminate mitigation/remediation guidance throughout the organization.
g. Ensure participation in any meetings, to include travel for any assessment, pre-audit, audit, and post-audit.

C.5.4.17 SUBTASK 17 – OPERATIONAL ORDERS (OPORDS) AND TASKINGS

The contractor shall support USACE OCIO/G-6 OPORDS and taskings. The Contractor shall:

a. Analyze and comply with assigned OPORDs/taskers within the assigned suspense date, making recommendations to service owners.
b. Review, draft, and obtain technical input for OPORDs, Fragmentary Orders, TASKORDs, and other system-requirements documentation.
c. Test and implement procedures to mitigate vulnerabilities or comply with other actions in the OPORD/tasker.
d. Develop POA&M and OISs within timelines of individual orders.
e. Track all assigned OPORDs/taskers and approved POA&Ms until completion and acceptance by the Government.

C.5.5 TASK 5 – TELECOMMUNICATIONS

USACE requires ongoing, scalable telecommunications services. The contractor shall provide a full range of telecom voice and data enterprise wired and wireless connectivity and services that provide connectivity to each USACE identified site. During TO performance, the need to establish services at additional locations will occur, as well as the need to terminate services at various locations, and the TO TDL process identified in **Section H.15** shall apply. The contractor shall also provide secure, reliable transport of agency applications across a high-speed, unified, multi-service IP-enabled backbone infrastructure. The contractor shall develop and maintain a Telecommunications Management Plan (TMP) detailing the status of services (i.e. Circuits, Devices, Mobile, etc.) at each location and any planned updates or changes **(Section F, Deliverable 56)**. USACE customers and end users at main offices, field sites, and vessels rely on this technology to accomplish mission tasks. Additionally, some users rely on remote wireless access, and the contractor shall support as required.

For each telecommunications support area, the contractor shall:

a. Continually monitor current commercially available service offerings and technology advancements, and make recommendations to USACE for implementation.
b. Ensure all designs and implementations provide customers appropriate bandwidth, latency, interoperability, etc., that enables uninterrupted voice, video, and data technologies at any USACE location. Procure all necessary infrastructure components and service plans.
c. Ensure designs and implementations are in accordance with DoD, Army, USACE, and industry standards and best practices where USACE standards do not currently exist.
d. Coordinate service delivery with other services providers to ensure seamless service to USACE end users.

C.5.5.1 SUBTASK 1 – TELECOMMUNICATIONS EXPENSE MANAGEMENT (TEM)

The contractor shall provide a total solution for expense management for the entire USACE wired, wireless, voice, and data environment to optimize the enterprise operating expenses. The contractor shall provide contract administration, inventory management, invoice management, audit services, call detail report services, rate plan optimization, advanced analysis and reporting, contract optimization, ordering and procurement services, dispute management and recovery, help desk, and transition services. The contractor shall make TEM information available through the contractor-provided portal. Expense information shall be available by district, site, office, function, and user level as appropriate to support analysis.

C.5.5.2 SUBTASK 2 – MOBILE COMMUNICATIONS SOLUTION

The contractor shall develop, plan, and implement an efficient, effective, and comprehensive mobile communications solution that provides all USACE users (CONUS and OCONUS) access to the most effective current, Government-approved commercially available service offerings (network, device, or other technology). The mobile communications solution shall be scalable (devices and network capability) and enhance the ability of USACE end users to conduct business.

The contractor shall assume operation of the current Government owned MDM solution and after award the contractor is expected to propose and ultimately provide a Mobile Device Management (MDM) solution that encompasses complete service lifecycle. The MDM solution shall include the limited provisioning of mobile devices technical support, activation of mobile communications plans (voice and data) deactivation of mobile communications plans, and any requisite additions, moves, or changes, and the eventual refresh, replacement, and disposal of mobile devices. The MDM solution shall be capable of provisioning mobile devices and services provided by other separate USACE contract vehicles. When service and devices are not provided separately, the RITS provider shall coordinate directly with regional or local carriers to meet USACE requirements. The contractor shall ensure its solutions provide customers appropriate bandwidth, latency, and interoperability to carry out mission-related activities. The contractor's solution may provide a complex and comprehensive strategy utilizing the services of multiple vendors to optimize services in different locations to maintain effective service levels. However,

at a minimum, service agreements shall be at the district level and also include international capability and compatibility.

The contractor's MDM solution shall provide integrated functionality with the USACE enterprise's applications to maximize end-user productivity and access. The end user/customer interface for the MDM solution shall be the IT service desk and contained in the contractor's portal solution. The contractor shall provide management-level information for enterprise mobile device usage and metrics.

C.5.5.3 SUBTASK 3 – AUDIO/WEB CONFERENCING AND CASTING SERVICES (AWCCS)

USACE OCIO/G-6 requires reservation less AWCCS available to all USACE end users to meet, present, and interact with information via a web browser, thereby allowing end users to share audio, video, information, documents, or applications interactively via the internet and the agency's intranet for audiences ranging from 2 to 50,000 geographically distributed participants.. A method to ensure content protection and authenticate users shall be included. This service shall have the ability to record sessions. The contractor shall continually update and maintain these services to remain current with commercial technology.

C.5.5.4 SUBTASK 4 – NETWORK CONNECTIVITY SOLUTION

The contractor shall develop, plan, acquire on behalf of USACE, install, and manage innovative, high-performance connectivity solutions for USACE networks. This includes various connection topologies, including wired and wireless (cellular, microwave, Satellite Communication (SATCOM)), reach-back at both common (district/division) and non-standard locations (hydroelectric stations, parks, locks, dams, etc.). Service connectivity can be delivered using various combinations of IP transport media. (e.g., copper, fiber, Wi-Fi, cable, cellular, satellite). Individual connections shall be consolidated at locations to be determined by the provider (meet-me type co-located facilities). These connection points shall require high speed/high bandwidth/low latency connections to the internet, alternate networks (DoDIN, SIPRs) and cloud providers, external telecom providers, and content delivery providers. This core infrastructure shall be designed as a multi-carrier environment with diverse multiple connections. Route/carrier diversity is envisioned to minimize impact from any nationwide and regional outages. Additionally, incorporating "last- mile," diverse on-site fiber entry is envisioned to minimize impact from any local fiber cuts or central office equipment failures. All contractor-provided connectivity solutions shall support analog- and IP-based voice services, and the contractor shall modernize existing connections to Ethernet-based (public or private) transport to increase service performance as required.

The combined core infrastructure and vendor-owned consolidation points (meet me co-location) shall provide worldwide access using technologies such as carrier-agnostic Software Defined Wide Area Network (SD-WAN), bandwidth on demand, remote access (VPN) software clients, and support of zero-trust environments.

Government-provided services such as Iridium, DoDIN, SIPRNet, Broadband Global Area Network (BGAN), Inmarsat, Short Burst Data, DSN, very-small-aperture terminal (VSAT) Bandwidth, Joint Worldwide Intelligence Communications System (JWICS), etc., will be

directly coordinated with the Government team for Designated Agency Representative (DAR)-related processing/actions.

C.5.6 TASK 6 – TRANSFORMATION

The USACE OCIO/G-6 environment is a dynamic, ever-changing environment, supporting the USACE global mission. In response to an evolving landscape, and in support of the USACE OCIO/G-6 strategic goals and objectives, the contractor shall provide transformation support that includes development of business processes and enterprise IT solutions, including innovative and emergent technologies focused on meeting overall objectives.

The contractor shall provide a dedicated workforce tasked with innovative, continual business process improvements leveraging advancements in technology and best industry practices to support the missions of the USACE and deliver service improvement. Transformations may begin as the result of a Government-identified problem or requirement or as a contractor-presented solution to a USACE mission. Transformation is designed to ensure process improvement is consistent, deliberate, and predictable. The contractor shall develop and deliver proposed innovations to the Government via a USACE led Innovation Review Board for review and approval. Approved innovations will be submitted to the FEDSIM COR for approval prior to implementation **(Section F, Deliverable 57)**.

C.5.6.1 SUBTASK 1 - PROVIDE STRATEGIC PLANNING SERVICES

The contractor shall provide recommendations on the design, development, implementation, and maturation of IT service management, not only as an organizational capability, but also as a strategic asset. The contractor shall provide recommendations on the principles underpinning the practice of IT service management to aid the development and modernization of USACE OCIO/G-6 service management policies, guidelines, and processes. The contractor shall assist the USACE OCIO/G-6 in translating IT strategic goals, commitments, and objectives into actionable plans, tasks, activities, technology, and/or process solutions and possible alternatives, including the estimated costs for the various options, and the potential risks associated with each alternative. The contractor shall develop and implement IT service management plans, practices, infrastructures, and systems utilizing industry best practices to optimize enterprise-wide IT service delivery and improve operational performance with minimal impact on the IT enterprise

C.5.7 TASK 7 – EMERGENCY RESPONSE

USACE provides support to the FEMA and other Federal, state, local, and tribal entities during national and natural emergency response and recovery operations. USACE OCIO/G-6 emergency response services provide IT capabilities in support of operations other than war (e.g., disaster relief, defense support to civil authorities, and foreign humanitarian assistance). Such services are primarily in support of emergencies or contingency operation and also directly support the Enterprise Emergency Response Team. The Enterprise Emergency Response Team uses Fly-Away Kits (FAK) consisting of CorpsNet components that augment existing services to provide a mobile virtual CorpsNet environment for emergency or contingency response. A single FAK contains hardware and software for switches, routers, VPN, and WAN equipment and associated spares.

The contractor shall support USACE's emergency response mission by providing emergency response IT services within the scope of this requirement and related emergency event planning and support to USACE. Deployed personnel shall have privileged access to USACE systems.

The contractor is required to have staff in travel status within 12 hours of Government notification and approval both OCONUS and CONUS. The contractor is expected to make all travel arrangements and be prepared to work as long as it takes in potentially austere environments.